UNITED STATES DISTRICT COURT

EASTERN DISTRICT OF WISCONSIN

In the Matter of the Seizure of
(Address or brief description of property or premises to be seized)

SEVEN DOMAIN NAMES THAT ARE STORED AT PREMISES OWNED, MAINTAINED, CONTROLLED, OR OPERATED BY VERISIGN, INC. – NAMELY, GSCONNECTS.COM, APPROVECONNECTS.COM, G3N3SIS.NET, GENESIS-UPDATE.NET, GENESIS-SECURITY.NET, GEN2DEV.NET, AND TRACECONTROL.NET

Case Number: 23-M-367 (SCD)

APPLICATION FOR A WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

I, [redacted] being duly sworn depose and say:

I am a Special Agent with the Federal Bureau of Investigation, and have reason to believe that in the Eastern District of Virginia there is now certain property – namely, the following seven domain names that are stored at premises owned, maintained, controlled, or operated by VeriSign, Inc.: gsconnects.com, approveconnects.com, g3n3sis.net, genesis-update.net, genesis-security.net, gen2dev.net, and tracecontrol.net – that is civilly forfeitable under 18 U.S.C. § 1030(j)(1), and criminally forfeitable under 18 U.S.C. §§ 1028(b)(5), 1029(c)(1)(C), and 1030(i)(1)(A), as property that is used in and/or intended to be used in facilitating and/or committing violations of 18 U.S.C. §§ 1028 (identity theft), 1029 (access device fraud), and 1030 (computer fraud), and which property is therefore also subject to criminal seizure under 21 U.S.C. § 853(f).

The application is based on these facts:

✓ Continued on the attached sheet.

❑ Delayed notice of ____ days (give exact ending date if more than 30 days:_____ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

[redacted]
Signature of Affiant

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone and email.

3-30-23. 2:05 pm
Date and time issued

at Milwaukee, Wisconsin
City and State

Stephen C. Dries, U.S. Magistrate Judge
Name & Title of Judicial Officer

Stephen C. Dries
Signature of Judicial Officer

AFFIDAVIT IN SUPPORT OF SEIZURE WARRANT

I, [redacted] being duly sworn, hereby declare as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a seizure warrant for the following domains, which are also listed in Attachments A-1 through A-3: Genesis.market ("Subject Domain 1"), g3n3sis.pro ("Subject Domain 2"), g3n3sis.org ("Subject Domain 3"), gsconnects.com ("Subject Domain 4"), approveconnects.com ("Subject Domain 5"), tracecontrol.net ("Subject Domain 6"), gen2dev.net ("Subject Domain 7"), g3n3sis.net ("Subject Domain 8"), genesis-update.net ("Subject Domain 9"), genesis-security.net ("Subject Domain 10"), and [redacted] ("Subject Domain 11") (collectively, the "Target Properties"). Subject Domains 4, 5, 6, 7, 8, 9, and 10 are stored at premises owned, maintained, controlled, or operated by VeriSign, Inc. ("VeriSign"). Subject Domains 1, 2, and 11 are stored at premises owned, maintained, controlled, or operated by Identity Digital Inc. ("Identity Digital"). Subject Domain 3 is stored at premises owned, maintained, controlled, or operated by Public Interest Registry ("PIR"). VeriSign, Identity Digital, and PIR are all electronic communication service providers and/or remote computing service providers. VeriSign is a domain registry in the United States and is headquartered, and accepts service of process, at 12061 Bluemont Way, Reston, Virginia. Identity Digital is a domain registry in the United States and is headquartered, and accepts service of process, at 10500 NE 8th Street, Suite 750, Bellevue, WA 98004. PIR is a domain registry in the United States and is headquartered, and accepts service of process, at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, VA 20190.

2. I am a Special Agent ("SA") for the Federal Bureau of Investigation ("FBI"). I have been employed by the FBI since June 2014, and I have been an SA since September 2017. I

am currently assigned to the FBI Milwaukee Division's Cyber Crime Task Force. As an SA for the FBI, I investigate criminal computer intrusion matters involving botnets, distributed denial of service attacks, the use of malware, identity theft, and other cyber national security matters. Prior to becoming an SA, I worked for the FBI as a staff operations specialist for approximately three years. As a staff operations specialist, I provided tactical analysis support to SAs working on cyber investigations involving national security issues.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

BACKGROUND REGARDING DOMAIN NAMES

4. Based on my training and experience and information learned from others, I am aware of the following:

5. **Internet Protocol (IP) Address**: An Internet Protocol address ("IP address") is a unique numeric address used by devices on the Internet. Every device attached to the Internet must be assigned a public IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. An IP address acts much like a home or business street address—it enables devices connected to the Internet to properly route traffic to each other. Devices connected to the Internet are assigned public IP addresses by Internet service providers ("ISPs"). There are two types of IP addresses: IPv4 (Internet Protocol version 4) and IPv6 (Internet Protocol version 6). An IPv4 address has four sets ("octets") of numbers, each ranging from 0 to 255, separated by periods (*e.g.*, 149.101.82.209). An IPv6 address has eight

groups ("segments") of hexadecimal numbers, each ranging from 0 to FFFF, separated by colons (*e.g.*, 2607:f330:5fa1:1020:0000:0000:0000:00d1).

6. **Domain Name**: A domain name is a string of text that maps to an IP address and serves as an easy-to-remember way for humans to identify devices on the Internet (*e.g.*, "justice.gov"). Domain names are composed of one or more parts, or "labels," delimited by periods. When read right-to-left, the labels go from most general to most specific. The right-most label is the "top-level domain" ("TLD") (*e.g.*, ".com" or ".gov"). To the left of the TLD is the "second-level domain" ("SLD"), which is often thought of as the "name" of the domain. The SLD may be preceded by a "third-level domain," or "subdomain," which often provides additional information about various functions of a server or delimits areas under the same domain. For example, in "www.justice.gov," the TLD is ".gov," the SLD is "justice," and the subdomain is "www," which indicates that the domain points to a web server.

7. **Domain Name System**: The Domain Name System ("DNS") is the way that Internet domain names are located and translated into IP addresses. DNS functions as a phonebook for the Internet, allowing users to find websites and other resources by their names while translating them into the IP addresses that their computers need to locate them.

8. **DNS Servers**: Domain Name Servers ("DNS servers") are devices or programs that convert, or resolve, domain names into IP addresses when queried by web browsers or other DNS "clients."

9. **Registrar**: A registrar is a company that has been accredited by the Internet Corporation for Assigned Names and Numbers ("ICANN") or a national country code top-level domain (such as .uk or .ca) to register and sell domain names. Registrars act as intermediaries

between registries and registrants. Registrars typically maintain customer and billing information about the registrants who used their domain name registration services.

10. **Registry**: A domain name registry is an organization that manages top-level domains, including by setting usage rules and working with registrars to sell domain names to the public. For example, the registry for the ".com" and ".net" top-level domains is VeriSign.

11. **Registrant**: A registrant is the person or entity that holds the right to use a specific domain name sold by a registrar. Most registrars provide online interfaces that can be used by registrants to administer their domain names, including to designate or change the IP address to which their domain name resolves. For example, a registrant will typically "point" their domain name to the IP address of the server where the registrant's website is hosted.

12. **Virtual Private Network (VPN)**: A virtual private network ("VPN") is software configured on a server that allows users to secure an encrypted connection over the Internet. This connection masks a user's true IP address by allowing the user to connect to the Internet via IP addresses that are owned by the VPN provider. These VPN-owned IP addresses are usually located all over the world. In other words, a VPN can make it so that a VPN user's Internet traffic is encrypted and also make it appear as though the VPN user is connecting from a VPN in another location. For example, if a VPN user is located in Germany, that VPN user can select a VPN IP address in another country (*e.g.*, the United States).

13. **WHOIS**: WHOIS is a protocol used for querying databases that store registration and other information about domains, IP addresses, and related Internet resources. For example, results from a WHOIS search of a domain would likely include contact information for the registry, the registrar, and the ISP that owns the IP address to which the domain points. Contact information for the registrant of the domain might be provided but is often redacted, masked, or inaccurate.

BACKGROUND REGARDING VIRTUAL CURRENCY

14. **Virtual Currency**: Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies, such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin (or "BTC") is currently the most well-known virtual currency in use.

15. **Virtual Currency Address**: Virtual currency addresses are the particular virtual locations to or from which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers.

16. **Blockchain**: The code behind many virtual currencies requires that all transactions involving that virtual currency be publicly recorded on what is known as a blockchain. The blockchain is essentially a distributed public ledger, run by a decentralized network of computers, containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies.

17. **Blockchain Analysis:** It is virtually impossible to look at a sole transaction on a blockchain and immediately ascertain the identity of the individual behind said transaction. That is because blockchain data generally only consists of alphanumeric strings and timestamps. That said, law enforcement can obtain leads regarding the identity of the owner of an address by analyzing blockchain data to figure out whether that same individual is connected to other relevant addresses on the blockchain. To do so, law enforcement can use blockchain explorers, as well as

commercial services offered by several different blockchain-analysis companies. These companies analyze virtual currency blockchains and attempt to identify the individuals or groups involved in transactions. "For example, when an organization creates multiple [BTC] addresses, it will often combine its [BTC] addresses into a separate, central [BTC] address (*i.e.*, a "cluster"). It is possible to identify a 'cluster' of [BTC] addresses held by one organization by analyzing the [BTC] blockchain's transaction history. Open-source tools and private software products can be used to analyze a transaction." *United States v. Gratkowski*, 964 F.3d 307, 309 (5th Cir. 2020). Through numerous unrelated investigations, law enforcement has found the information provided by these tools to be reliable.

CASE BACKGROUND AND EVIDENCE ESTABLISHING PROBABLE CAUSE TO SEIZE SUBJECT DOMAIN 1

18. Since approximately August 2018, the FBI has been investigating an illicit online marketplace named Genesis Market. Genesis Market is a private marketplace that is primarily hosted at the Internet domain "genesis.market" (Subject Domain 1). Genesis Market's operators compile stolen data (*e.g.*, computer and mobile device identifiers, email addresses, usernames, and passwords) from malware-infected computers around the globe and package[1] it for sale on the market.[2]

19. These packages generally allow a criminal actor to masquerade as a victim and allow the criminal actor to trick a third-party company's anti-fraud detection system into granting

[1] Genesis Market refers to these packages of stolen data as "bots" on their site; however, typically, an Internet bot refers to a piece of software that runs automated tasks over the Internet. Since Genesis Market's use of the word "bot" strays from the normal meaning, the term "package" is used throughout this request.

[2] Malware, or malicious software, is any piece of software that is written to damage and/or steal data from an Internet connected device. Viruses, trojans, spyware, and ransomware are all different types of malware.

the criminal actor access to the application or website. As a result, Genesis Market is one of the most prolific initial access brokers (IABs)[3] in the cybercrime space. In general, IABs attract criminals, such as ransomware actors, looking to expedite infiltration into, and lateral movement within, a targeted system. Speeding up those steps reduces the time required to attack a victim network and minimizes detection by software installed to protect networks against malicious intrusions.

20. As of on or about March 2023, there were approximately 460,000 packages listed for sale on Genesis Market. Each package represents a single, compromised computer or device. According to Genesis Market's website, the packages are located across North America (including in the Eastern District of Wisconsin), Europe, South America, and parts of Asia.

21. Over the course of the last four years, the FBI has observed that the packages of stolen data are generally searchable based on areas of interest (*e.g.*, banking information, social media accounts, etc.), country of origin, price, and the date of infection (*i.e.*, the date the victim device was infected with malware). The prices of the packages vary and depend, primarily, on three factors: (1) the number of online accounts ("resources") associated with the package (*e.g.*, accounts with legitimate credentials for platforms like Amazon, Netflix, Gmail, etc., are more valuable); (2) how recently the package was compromised; and (3) whether there is a "fingerprint" associated with the package. A fingerprint is a group of identifiers that third-party applications or websites use to identify a computer or device. These fingerprints allow the applications or websites to confirm that the device is a trusted source. The FBI has determined that in situations where a fingerprint is associated with a package, Genesis Market provides the purchaser with a proprietary

[3] IABs sell access to compromised networks so that cybercriminals do not need to spend time finding compromised systems. Instead, those cybercriminals can use IABs as a shortcut and deploy their own malware immediately after they have victim information from the IABs.

plugin (*i.e.*, an Internet browser extension that provides additional functionality). This proprietary plugin amplifies that purchaser's ability to control and access the package's data.

GENESIS MARKET'S CONNECTIONS TO THE EASTERN DISTRICT OF WISCONSIN

22. Since approximately September 19, 2018, the FBI has funded (via BTC transactions) the purchase of approximately 115 packages on Genesis Market. The FBI has reviewed the data from purchased packages and determined that Genesis Market works as advertised: it is, in fact, collecting and selling victims' personal identifying information around the world. Of those packages purchased by the FBI, approximately 27 were stolen from computers located in Wisconsin, approximately seven of which were located in the Eastern District of Wisconsin. Agents showed victim computer owners in the Eastern District of Wisconsin the usernames and passwords that the agents had obtained via the Genesis Market, and the victims confirmed that the usernames and passwords belonged to them and had been stolen.

TRACING THE BTC ADDRESSES ASSOCIATED WITH GENESIS MARKET AND FURTHER EVIDENCE TIED TO SUBJECT DOMAIN 1

23. As explained above, the FBI has funded the purchase of approximately 115 packages on Genesis Market. Those purchases were made using BTC, which is traceable along the BTC blockchain. Additionally, as part of this investigation, FBI agents have reviewed records from a hosting provider ("Hosting Provider 1"). Hosting Provider 1 was the hosting provider for the server and IP address associated with genesis.market, which is Subject Domain 1 (*i.e.,* the server provider that Genesis Market's administrators are paying to host Subject Domain 1 so that Subject Domain 1 can remain active on the Internet). Those records from Hosting Provider 1 revealed that three BTC addresses were associated with the registration of Subject Domain 1 (*i.e.*, those BTC addresses were used to pay Hosting Provider 1 for the use of the server that resolves to the Subject

Domain 1). While conducting blockchain analysis to trace the transactions associated with those three BTC addresses, FBI agents observed that portions of those BTC payments for Hosting Provider 1 services made their way to or through a BTC address ending "J43QW" ("BTC Address 1"). The analysis further revealed that BTC Address 1 sent approximately 20 payments to merchants who used a U.S.-based BTC payment processer ("BTC Payment Processor 1"). Those 20 payments each have a unique "transaction ID" associated with them.

24. In or around September 2019, BTC Payment Processor 1 (in response to legal process) provided the FBI with subscriber information related to the 20 payments from BTC Address 1. These records from BTC Payment Processor 1 included information about the merchant associated with each transaction ID, as well as information about the buyer, such as the buyer's name, physical address, and/or email address. BTC Payment Processor 1's records revealed that one of the 20 transactions was conducted via IP address 185.214.10.128, by an individual listed on the BTC Payment Processor 1 records as "Kenneth GXXXXXki," from Tempe, Arizona, and the email address "mmarora@XXX.de."[4] Investigators reviewed additional records that indicated IP address 185.214.10.128 was owned by a hosting provider that specializes in virtual private server ("VPS") services ("Hosting Provider 2"). A VPS is a virtual machine sold as a service by an Internet hosting provider.

SEARCH WARRANT FOR GENESIS MARKET-RELATED DATA FROM HOSTING PROVIDER 2

25. Based, in part, on the foregoing, a search warrant was issued for information held by Hosting Provider 2. Records from Hosting Provider 2 confirmed that BTC Address 1 was used to pay Hosting Provider 2 for use of a server that was acting as a proxy server for Genesis Market.

[4] Throughout this affidavit, names and other personal identification information have been redacted, using the letter "X," as a means of avoiding the revelation of any sensitive information.

Proxy servers act as intermediaries for requests from a "client" (*i.e.*, a computer that connects to and uses the resources of a remote computer or server) to a server. Based on my training and experience, I know that cybercriminal actors often use a combination of proxy servers and virtual private networking to obfuscate the location of their hosting infrastructure and to avoid law enforcement detection.

26. Here, I believe that Genesis Market's administrators used a VPS server owned by Hosting Provider 2 as a means of concealing the true location of Genesis Market's backend servers (*i.e.*, the server(s) responsible for storing and organizing data to ensure everything on the client-side of a website actually works). While reviewing the Hosting Provider 2 data obtained via the above-referenced warrant, investigators found that this VPS server was forwarding Internet traffic to a server hosting IP addresses 62.138.8.171 and 85.25.203.178 (the "Genesis Backend #1 IP Addresses"), which shared the same SSL certificate[5] (the "Genesis Backend #1 SSL Certificate"), meaning that both IP addresses were likely controlled by the same individual(s).[6] As explained further below, investigators later confirmed that the server hosting the Genesis Backend #1 IP Addresses was the backend server of Genesis Market.

[5] A Secure Sockets Layer ("SSL") certificate is a digital certificate that authenticates the identity of a website and encrypts information sent to the server. An SSL certificate contains the following information: certificate holder's name; the certificate's serial number and expiration date; a copy of the certificate holder's public key; and the digital signature of the certificate-issuing authority. If one is dealing with information that requires encryption (*e.g.*, payment or other personal information), a website operator needs an SSL certificate.

[6] Based on my training and experience, I know that only a user with administrative privileges to both Genesis Backend #1 IP Addresses and to the Genesis Backend #1 SSL Certificate would be able to associate the SSL Certificate with specific IP addresses.

SERVER DATA ASSOCIATED WITH THE GENESIS BACKEND SERVER #1

27. On or about December 9, 2020, the FBI, with assistance from a foreign law enforcement partner, obtained a forensic image of the server hosting the Genesis Backend #1 IP Addresses. Based on analysis of that forensic image, the FBI confirmed that this server was hosting Genesis Market's backend (the "Genesis Backend Server #1"), as the FBI found voluminous records on that server associated with Genesis Market's operations. For example, the server contained, among other things, usernames; passwords; email accounts; Jabber[7] accounts; BTC addresses; user search history; user purchase history; user tickets and comments; and records of packages sold or displayed for sale on Genesis Market. The FBI reviewed this data and found (1) that as of on or about December 7, 2020, there were approximately 33,000 Genesis Market users and approximately 900,000 individual packages (or "bots") that had been listed for sale or sold on Genesis Market, and (2) that more than $4,000,000 dollars' worth of virtual currency had been deposited into Genesis Market.

28. Shortly after investigators obtained the forensic image of the Genesis Backend Server #1, Genesis Market went offline. The investigation further found that during this downtime, the administrators of Genesis Market changed their hosting infrastructure (*i.e.*, leased new servers and associated the market with different IP address, among other things). Thereafter, the FBI continued to work to identify the infrastructure supporting Genesis Market, and in or around January 2022, determined that Genesis Market's new backend server was located outside of the United States. In or around May 2022, with assistance from another foreign law enforcement partner, the FBI obtained a forensic image of the server that was hosting the then-active Genesis

[7] Jabber is an online messaging platform.

Market backend server (the "Genesis Backend Server #2). Analysis of that forensic image revealed that it contained much of the same information as the Genesis Backend Server #1, as well as updated user data and other information. For example, the data from Genesis Backend Server #2 showed the following about Genesis Market's activities from approximately 2018 through on or about May 18, 2022:

a. There were approximately 59,000 individual user accounts on Genesis Market.

b. There were approximately 1.5 million individual packages (or "bots") that had been compromised and advertised for sale on Genesis Market.

c. There were approximately 80 million account access credentials made available for sale on Genesis Market.

d. There were more than 200,000 account access credentials for sale on Genesis Market that were associated with federal, state, and local government accounts. [redacted]

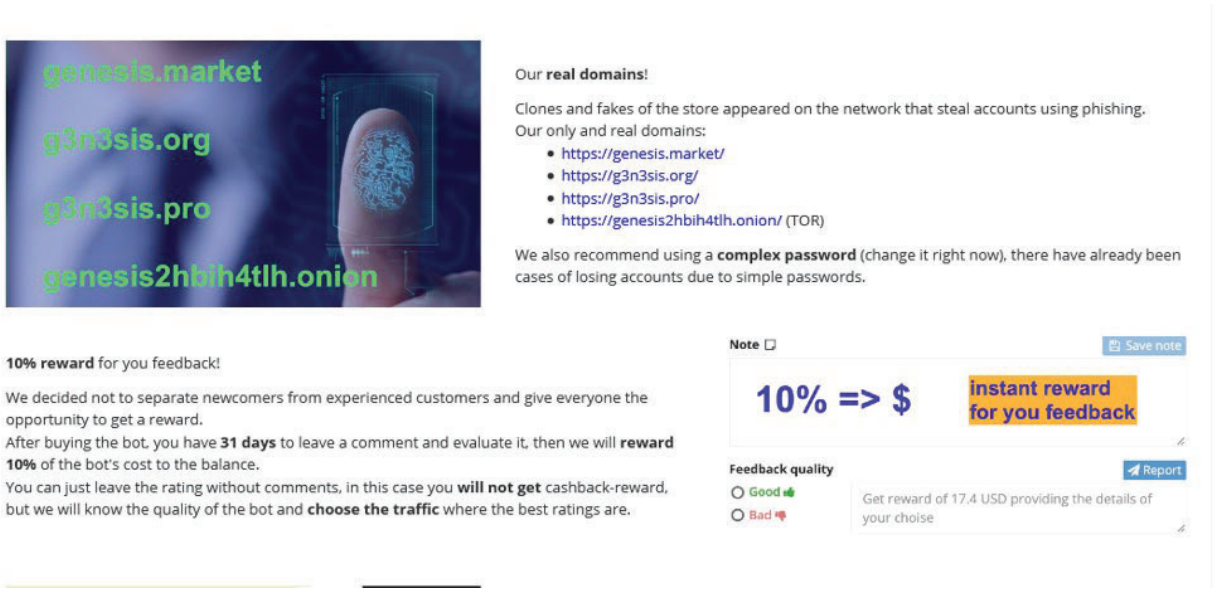
e. Genesis Market's users made more than $8 million dollars in virtual currency deposits to the market.

29. Based on the information obtained from the Genesis Market backend servers (Genesis Backend Server #1 and Genesis Backend Server #2), as well as other information obtained throughout the course of the investigation, I believe that Genesis Market has been used to facilitate wide-scale fraud on individuals, companies, governments, and other entities around

the world, as well as numerous ransomware incidents, thefts of intellectual property, and other cybercrimes.

EVIDENCE ESTABLISHING PROBABLE CAUSE TO SEIZE SUBJECT DOMAINS 1-6

30. In or around October 2021, the Genesis Market operators posted on the Genesis Market website that the legitimate clear web domains for Genesis Market (*i.e.*, websites accessible from traditional browsers, as opposed to those used to access the dark web[8]) were genesis.market (Subject Domain 1), g3n3sis.pro (Subject Domain 2), and g3n3sis.org (Subject Domain 3). The posting, as shown in the below screenshot, was still listed in the "News" section for Genesis Market as of on or about March 13, 2023, noting that it was posted "a year ago."



31. Notably, since in or around January 2021, through in or around November 2022, Subject Domain 2, Subject Domain 3, Subject Domain 4 (gsconnects.com), Subject Domain 5 (approveconnects.com), and Subject Domain 6 (tracecontrol.net) have followed Subject Domain

[8] The "dark web" is the part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable. One way to access the dark web is via an Internet browser named "Tor," which is short for "The Onion Router."

1's IP address movements. In other words, any IP address hosting the Subject Domain 1 was also hosting, at the same time, Subject Domain 2, Subject Domain 3, Subject Domain 4, Subject Domain 5, and Subject Domain 6. Since in or around November 2022, Subject Domain 2, Subject Domain 3, Subject Domain 5, and Subject Domain 6 have continued to be associated with the same IP address as Subject Domain 1. Since in or around November 2022, Subject Domain 4 has resolved to an IP address that appears to be "parked," meaning that it was not actively being used to host Genesis Market infrastructure. However, records show that Subject Domain 4 has not been resold or purchased, indicating that, based on my experience and understanding of domains, Genesis Market's administrators continue to own it. Records also show that the administrators continue to privacy-protect Subject Domain 4 through on or about December 29, 2023.[9]

32. The above-described IP address overlap demonstrates, based on my training and experience, that these domains are owned by the same individual(s). Further, over the course of this investigation, I performed a historical DNS lookup of Subject Domain 1, Subject Domain 2, and Subject Domain 3. Those historical DNS records, also known as passive DNS records, confirmed that Subject Domain 4, Subject Domain 5, and Subject Domain 6 are also connected to Genesis Market infrastructure. More specifically, as of on or about March 15, 2023, a WHOIS lookup of Subject Domain 1 showed that Subject Domain 1 resolved to IP address 176.124.192.48. Passive DNS records for IP address 176.124.192.48 showed that Subject Domain 2, Subject Domain 3, Subject Domain 5, and Subject Domain 6 also resolved to that IP address at the same time, meaning they were hosted on the same server.

[9] "Privacy Protection" is further explained later in this affidavit.

EVIDENCE ESTABLISHING PROBABLE CAUSE TO SEIZE SUBJECT DOMAINS 7 & 8

33. As previously discussed above, Genesis Market's administrators used a VPS server purchased from Hosting Provider 2 as a proxy server, which helped obfuscate the true location of Genesis Backend Server #1. While reviewing the Hosting Provider 2 data, investigators found that, in addition to forwarding traffic to the Genesis Backend Server #1, this proxy server was also connecting to a server hosting IP address 109.123.95.165 that was associated with the domain "gen2dev.net" (Subject Domain 7) (the "Gen2dev Server"). The FBI determined that the Gen2dev Server was also used for Genesis Market operations because, for among other reasons, data from the backend servers showed that the first "user" account of Genesis Market registered via the email address "client@gen2dev.net" in or around August 2017, which was several months before Genesis Market was "live" (*i.e.*, advertising and accessible by public users). Based on my training and experience, I know that the first "user" account registered on a marketplace is often created by an administrator for testing purposes. Additionally, the registrant information per open source WHOIS records and as found on DomainTools associated with Subject Domain 7 showed that the email registrant for Subject Domain 7 matched the email registrant for g3n3sis.net (Subject Domain 8).

34. Investigators queried the DNS records for Domain 7 and Domain 8 and found that as of in or around September 2022, the domain records had been deleted from Reg.ru, which was the Russian-based domain registrar for both domains. However, as of in or around July 2022, Domain 7 and Domain 8 were registered and paid for, with an expiration date of in or around July 2023. In other words, just because Genesis Market's administrators deleted the domain records does not mean that they no longer own the domains.

35. A review of Subject Domain 8's passive DNS history showed that Subject Domain 8 was registered on or about July 26, 2016, and initially had "Privacy Protection" in place. When a domain is registered, it is an industry standard to provide an additional service that redacts the registrant information (*e.g.*, name, address, email, phone number, and other identifiers associated to the domain registrant) from WHOIS records. This redaction service is often referred to as "Privacy Protection." Based on my training and experience, I know that use of Privacy Protection restricts law enforcement from being able to see registrant information without proper legal process. Access to that information becomes nearly impossible if the domain provider is within a country that typically does not honor US requests for such information, such as Russia. However, in order for Privacy Protection to continue to be associated with a domain, the Privacy Protection needs to be purchased every year (in most cases). If a user discontinues or forgets to re-register the privacy protection, it will eventually expire, allowing others, including law enforcement, to be able to see registrant information for the suspect.

36. Here, it appears, based on a recent review of these passive DNS records, that at some point the Genesis Market administrators either intentionally or unintentionally stopped paying the Privacy Protection service fee for Subject Domain 8. As a result, Subject 8 was no longer privacy protected and so I was able to see that the registrant email for the domain was mezina.svet@yandex.ru. This was the same registrant email used for gen2dev.net (Subject Domain 7). As a result, it is reasonable to believe that Subject Domain 7 and Subject Domain 8 were registered by the same person or group and, as indicated above, both are part of Genesis Market's hosting infrastructure. Based on my training and experience, I believe it is reasonable to conclude that the Genesis Market administrators likely deleted the registrar records associated with Subject Domain 7 and Subject Domain 8 because they were an operational security risk to Genesis Market,

in that they could lead law enforcement to figure out information regarding Genesis Market's hosting infrastructure.

EVIDENCE ESTABLISHING PROBABLE CAUSE TO SEIZE SUBJECT DOMAINS 9 & 10

37. In 2020 and 2021, Subject Domain 9 (genesis-update.net) and Subject Domain 10 (genesis-security.net) were connected to Genesis Market's hosting infrastructure via the naming convention (*i.e.*, the inclusion of "genesis" in the domain), as well IP address overlap. For example, in or around October 2020, Subject Domains 9 and 10 resolved to IP address 89.42.212.194. IP address 89.42.212.194 was a known Genesis Market IP address, in that it hosted, for a time, Subject Domain 1, Subject Domain 2, and Subject Domain 3. Additionally, in response to legal process, the DNS provider for Subject Domain 9 and Subject Domain 10 ("Hosting Provider 3") provided information showing that the DNS registration for Subject Domain 9 was created by a user listing email address silverXXXX@XXX.de and that the DNS registration for Subject Domain 10 was created by a user listing email address seaXXXX@XXXXX.ch. Both of these email addresses are associated with Genesis Market in other contexts. For instance, information from BTC Payment Processor 1 (discussed above) showed that a user with the email address seaXXXX@XXXXX.ch. made a purchase connected to BTC Address 1 (discussed above), and that silverXXXX@XXX.de was used to register a proxy service used by Genesis Market administrators.

38. The evidence establishes that the decommissioning of Subject Domain 9 and Subject Domain 10 by Genesis Market on or around January 2021 was likely purposeful, as Subject Domain 4 and Subject Domain 5 were created at the end of December 2020 (*i.e.*, after the FBI acquired the data associated with Genesis Backend Server #1). The collection of this data by FBI may have been an indication to the Genesis Market operators that Subject Domain 9 and Subject Domain 10 were compromised by those law enforcement actions. Based on my training and

experience, I believe that switching domains, but keeping Privacy Protection in place, would likely be seen as a way for Genesis Market operators to attempt to avoid discovery by law enforcement and/or additional law enforcement actions.

39. Based on a review of passive DNS records, it appears that in or around October 2021, Genesis Market administrators stopped associating with new IP addresses Subject Domain 9 and Subject Domain 10 with current Genesis Market IP infrastructure; however, as of on or about March 13, 2023, WHOIS records show that the Privacy Protection for Subject Domain 9 and Subject Domain 10 is active until February 5, 2024. This indicates that the users controlling Subject Domains 9 and 10 intend to keep control of the domains well into the future, as they are not only paying to keep the domains registered, but they also have paid for Privacy Protection until 2024. Thus, even though the domains are not currently facilitating Genesis Market's operations, they remain in the administrators' control and could be used in the future.

EVIDENCE ESTABLISHING PROBABLE CAUSE TO SEIZE SUBJECT DOMAIN 11

40. [redacted]

[redacted]

10 [redacted]

41. [redacted]

42. [redacted]

STATUTORY BASIS FOR SEIZURE AND FORFEITURE

43. I respectfully submit that there is probable cause to believe that multiple subjects of this investigation have committed violations of, inter alia, 18 U.S.C. §§ 371 (conspiracy to

[redacted]

commit a federal offense), 1028 (identity theft), 1029(a)(2) (trafficking access devices), 1030(a)(2) (illegally accessing a protected computer), 1030(a)(5) (illegally damaging a protected computer), 1030(b) (conspiracy to commit computer fraud), and 1343 (wire fraud) (collectively, the "Subject Offenses")

44. I further submit that there is probable cause to believe that the Target Properties are subject to seizure and criminal forfeiture pursuant to:

a. Title 18, United States Code, Section 1028(b)(5), as personal property used, or intended to be used, to commit identity theft, in violation of Title 18, United States Code, Section 1028(a);

b. Title 18, United States Code, Section 1029(c)(1)(C), as personal property used, or intended to be used, to commit access device fraud, in violation of Title 18, United States Code, Section 1029(a); and

c. Title 18, United States Code, Section 1030(i)(1)(A), as personal property that was used, or intended to be used, to commit or to facilitate the commission of a Section 1030 violation.

45. Title 18, United States Code, Sections 1028(g), 1029(c)(2), and 1030(i)(2) specify that the forfeiture of such property, including seizure and disposition, is procedurally governed by Title 21, United States Code, Section 853.

46. To protect the ability of the United States to exercise its right of forfeiture, Title 21, United States Code, Section 853(e) empowers district courts to enter restraining orders and injunctions to preserve the availability of property that is subject to forfeiture under Section 853(a). However, if there is probable cause to believe that the property to be seized is subject to forfeiture and that an order pursuant to Section 853(e) may not be sufficient to assure its availability for

forfeiture, a district court may issue a warrant authorizing the seizure of such property. 21 U.S.C. § 853(f). Section 853(f) provides that:

> The Government may request the issuance of a warrant authorizing the seizure of property subject to forfeiture under this section in the same manner as provided for a search warrant. If the court determines that there is probable cause to believe that the property to be seized would, in the event of conviction, be subject to forfeiture and that an order under subsection (e) may not be sufficient to assure the availability of the property for forfeiture, the court shall issue a warrant authorizing the seizure of such property.

47. With regard to jurisdiction for issuance of a seizure warrant in this context, Section 853(l) provides that "district courts of the United States shall have jurisdiction to enter orders as provided in this section without regard to the location of any property which may be subject to forfeiture under this section. . . ."

48. Additionally, I submit that there is probable cause to believe that the Target Properties are subject to seizure and civil forfeiture pursuant to Title 18, United States Code, Section 1030(j)(1) as personal property that was used, or intended to be used, to commit or to facilitate the commission of a Section 1030 violation.

49. This application seeks a seizure warrant under both civil and criminal authority, because the property to be seized could easily be placed beyond process if not seized by warrant, as the Target Properties exist online and could be easily removed and/or destroyed by the subjects of the investigation. As previously stated, there is probable cause to believe that the Target Properties are subject to forfeiture because they were used to facilitate identity theft, access device fraud, and computer fraud, as well as contain evidence of those crimes. By seizing the Target Properties, the United States will prevent third parties from acquiring the Target Properties, as well as the information contained therein, and using them to for additional crimes.

SEIZURE PROCEDURE

50. As detailed in Attachments A-1 through A-3, upon execution of the seizure warrant, Identity Digital, PIR, and VeriSign shall be directed to restrain and lock the Target Properties, pending transfer of all right, title, and interest in the Target Properties to the United States, upon completion of forfeiture proceedings, to ensure that changes to the Target Properties cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the U.S. Department of Justice.

51. In addition, upon seizure of the Target Properties by the Government, Identity Digital, PIR, and VeriSign will be directed to associate the Target Properties to new authoritative name servers to be designated by a law enforcement agent. The Government will display a notice on the website to which the Target Properties will resolve, indicating that the sites have been seized pursuant to a warrant issued by this court.

CONCLUSION

52. For the foregoing reasons, I submit that there is probable cause to believe that the Target Properties are used in and/or intended to be used in facilitating and/or committing the Subject Offenses. Accordingly, the Target Properties are subject to criminal forfeiture under Title 18, United States Code, Sections 1028(b)(5), 1029(c)(1)(C), and 1030(i)(1)(A), and are subject to civil forfeiture under Title 18, United States Code, Section 1030(j)(1). The Target Properties are subject to criminal seizure under Title 21, United States Code, Section 853(f).

53. Because the warrant will be served on Identity Digital, PIR, and VeriSign, which control the Target Properties, and Identity Digital, PIR, and VeriSign, thereafter, at a time convenient to them, will transfer control of the Target Properties to the Government, there exists reasonable cause to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A-1

This warrant applies to the following domains:

(1) gsconnects.com

(2) approveconnects.com

(3) g3n3sis.net

(4) genesis-update.net

(5) genesis-security.net

(6) gen2dev.net

(7) tracecontrol.net

(collectively, the "Target Properties")

The Target Properties are stored at premises owned, maintained, controlled, or operated by VeriSign, Inc. ("VeriSign"), which accepts service of legal process at 12061 Bluemont Way, Reston, Virginia.

ATTACHMENT B-1

IT IS ORDERED that VeriSign, which is the provider for the property listed in Attachment A-1 (the Target Properties), shall take the following actions to effect seizure of the property identified in Attachment A-1:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation (FBI) by associating the Target Properties to the following authoritative name servers:
    a. jocelyn.ns.cloudflare.com;
    b. plato.ns.cloudflare.com; and
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to VeriSign.
2. Prevent any further modification to, or transfer of, the Target Properties, pending transfer of all right, title, and interest in the Target Properties to the United States, upon completion of forfeiture proceedings, to ensure that changes to the Target Properties cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the U.S. Department of Justice.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
5. The Government will display a notice on the website to which the Target Properties will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.
>
> To determine if you have been victimized, visit: haveibeenpwned.com or politie.nl/checkyourhack.
>
> Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov.

ATTACHMENT A-2

This warrant applies to the following domains:

(1) Genesis.market

(2) g3n3sis.pro

(3) [redacted]

(collectively, the "Target Properties")

The Target Properties are stored at premises owned, maintained, controlled, or operated by Identity Digital Inc. ("Identity Digital"), which accepts service of legal process at 10500 NE 8th Street, Ste. 750, Bellevue, WA 98004.

ATTACHMENT B-2

IT IS ORDERED that Identity Digital, which is the provider for the property listed in Attachment A-2 (the Target Properties), shall take the following actions to effect seizure of the property identified in Attachment A-2:

1. Take all reasonable measures to redirect the domain names to substitute servers at the direction of the Federal Bureau of Investigation (FBI) by associating the Target Properties to the following authoritative name servers:
    a. jocelyn.ns.cloudflare.com;
    b. plato.ns.cloudflare.com; and
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to Identity Digital.
2. Prevent any further modification to, or transfer of, the Target Properties, pending transfer of all right, title, and interest in the Target Properties to the United States, upon completion of forfeiture proceedings, to ensure that changes to the Target Properties cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the U.S. Department of Justice.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
5. The Government will display a notice on the website to which the Target Properties will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.
>
> To determine if you have been victimized, visit: haveibeenpwned.com or politie.nl/checkyourhack.
>
> Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov.

ATTACHMENT A-3

This warrant applies to the following domain:

(1) g3n3sis.org (the "Target Property")

The Target Property is stored at premises owned, maintained, controlled, or operated by Public Interest Registry ("PIR"), which accepts service of legal process at 11911 Freedom Drive, 10th Floor, Suite 1000, Reston, VA 20190.

ATTACHMENT B-3

IT IS ORDERED that PIR, which is the provider for the property listed in Attachment A-3 (the Target Property), shall take the following actions to effect seizure of the property identified in Attachment A-3:

1. Take all reasonable measures to redirect the domain name to substitute servers at the direction of the Federal Bureau of Investigation (FBI) by associating the Target Property to the following authoritative name servers:
    a. jocelyn.ns.cloudflare.com;
    b. plato.ns.cloudflare.com; and
    c. Any new authoritative name server or IP address to be designated by a law enforcement agent in writing, including email, to PIR.
2. Prevent any further modification to, or transfer of, the Target Property, pending transfer of all right, title, and interest in the Target Property to the United States, upon completion of forfeiture proceedings, to ensure that changes to the Target Property cannot be made absent court order or, if forfeited to the United States, without prior consultation with the FBI or the U.S. Department of Justice.
3. Take all reasonable measures to propagate the necessary changes through the Domain Name System as quickly as practicable.
4. Provide reasonable assistance in implementing the terms of this Order and take no unreasonable action to frustrate the implementation of this Order.
5. The Government will display a notice on the website to which the Target Property will resolve. That notice will consist of law enforcement emblems and the following text (or substantially similar text):

> Genesis Market's domains have been seized by the FBI pursuant to a seizure warrant issued by the United States District Court for the Eastern District of Wisconsin. These seizures were possible because of international law enforcement and private sector coordination involving the partners listed below.
>
> To determine if you have been victimized, visit: haveibeenpwned.com or politie.nl/checkyourhack.
>
> Been active on Genesis Market? In contact with Genesis Market administrators? Email us, we're interested: FBIMW-Genesis@fbi.gov.